Cyber Security Program Implementation Lessons Learned

Michael Bailey, Duke Energy Corporation
Jason Castro, Tennessee Valley Authority
William Gross, Nuclear Energy Institute

December 6, 2016 • Rockville, MD

History of Addressing the Cyber Threat

2002-2004

- NEI Cyber Security Task Force Formed
- Interim Compensatory Measures (ICM) Order
- Work Hours, Training and Revised DBT Orders
- NRC Completes Cyber Assessment Pilot Program
- NUREG\CR-6847, Cyber Security Self-Assessment Method

2005-2007

- NEI 04-04, Cyber Security Program for Power Reactors
- NRC Endorses NEI 04-04
- NEI, NERC MOA, NEI 04-04 Equivalent to CIPS 002-009
- NSIAC Voluntary Initiative for Cyber Security Programs
- RG 5.69, Design-Basis Threat
- Cyber Attack Added to Design Basis Threat

2008-2010

- NEI 04-04 Implemented
- NRC Cyber Rule Issued
- NRC Endorses NEI 08-09, Cyber Plan Template
- FERC Order 706-B Resolution – NRC rule covers balance of plant

2011-2013

- NRC Endorses Cyber Plan Implementation Schedule Template
- NRC Approves Plans
- Milestones 1-7 Implemented
- NRC Inspections Begin
- Presidential Executive Order and Policy Directive 21

2014-2017

- Cyber Event Notification Rule Issued and Implemented
- Full Program Implementation
- NRC Completes Initial Inspections
- NRC Begins Full Program Inspections

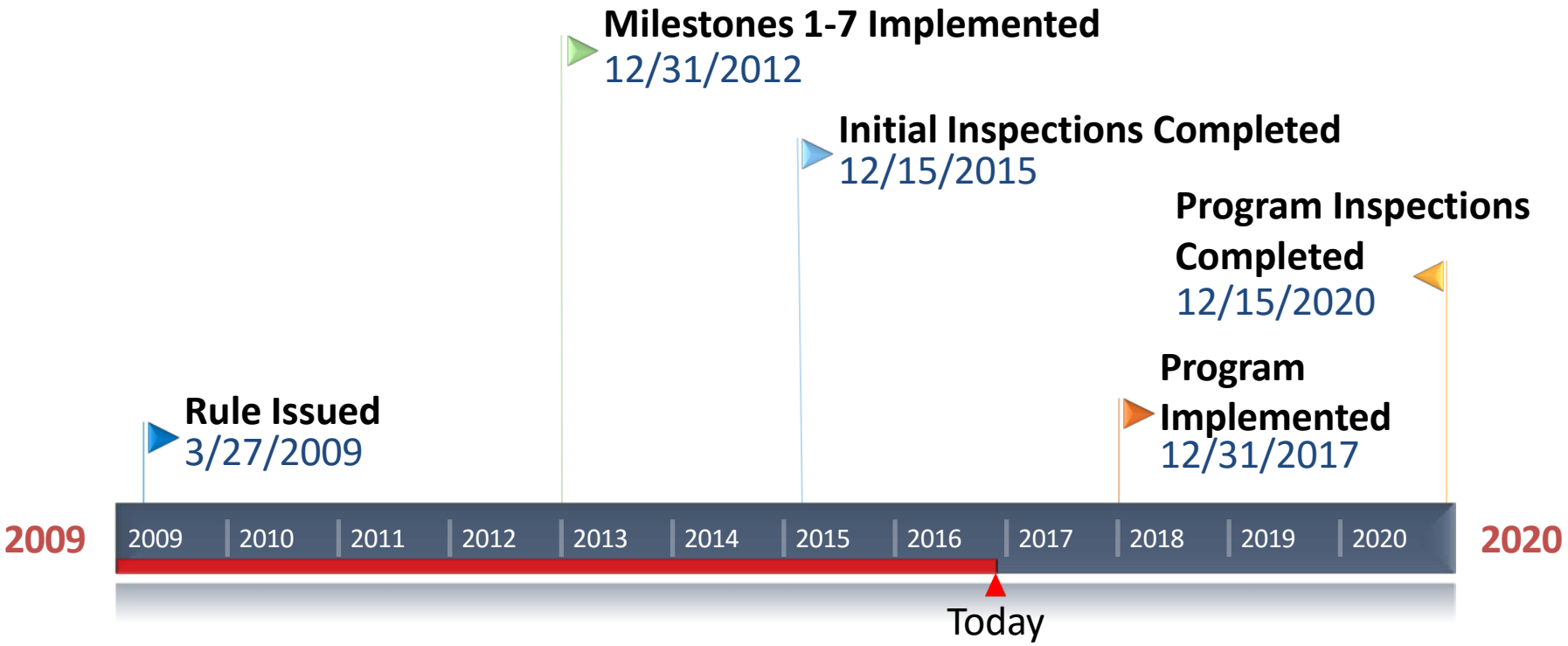
Measures Implemented by 12/31/2012

- Form a cyber security team
- Identify critical digital assets
- Isolate the plant from all network access
- Implement comprehensive controls over portable media and mobile devices
- Enhance insider mitigate programs
- Implement and maintain cyber controls for essential assets

Purpose, Objective, and Output

- Purpose
  - Review lessons learned from the implementation of cyber security requirements at U.S. reactors
- Objective – Use lessons learned to inform:
  - Remaining cyber program implementation
  - Future cyber security rulemaking efforts
- Output
  - Documented lessons learned, recommendations

Reactor Cyber Program Implementation



Ongoing Regulatory Activities

- Fuel cycle facilities
- Independent Spent Fuel Storage Facilities
- Decommissioning facilities
- Advanced reactors
- Part 37 Byproduct Materials

Lessons Learned - Development

- Team: NEI Cyber Security Task Force
  - All plants represented
  - Members have a wide range of areas of expertise
- Process: Facilitated discussion
  - Questionnaire provided
  - Several engagements in 2016 to elicit information

Lessons Learned - Scope

- Rulemaking and guidance development efforts
- Development of industry guidance and implementation schedule
- Implementation of Milestones 1-7
- Inspections of Milestone 1-7 implementations

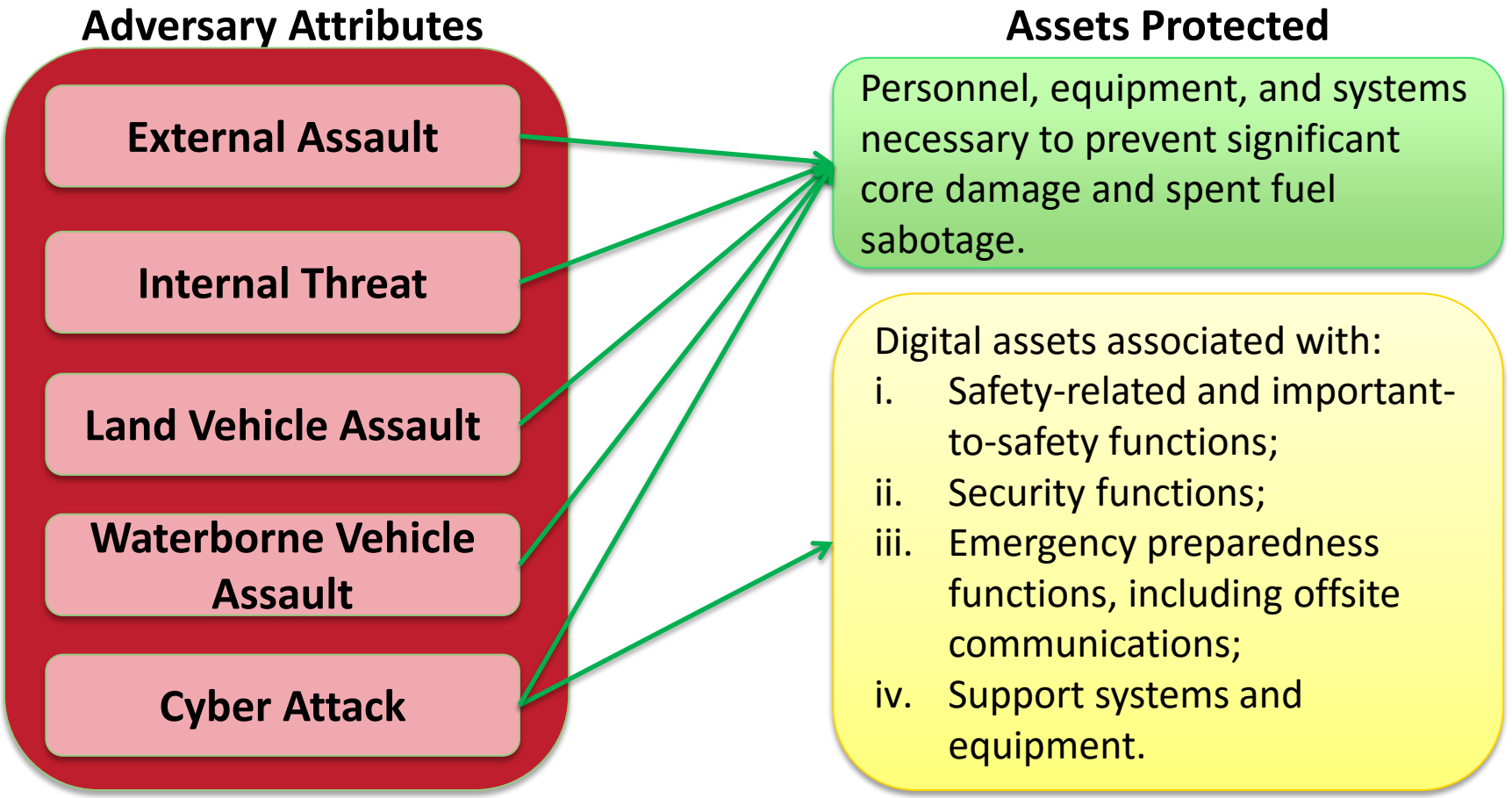
Lessons Learned Topical Areas

- Program Scope and Performance Objectives
- The Internal Threat
- Program Implementation
- Industry Support and Executive Oversight
- Inspections and NRC Oversight

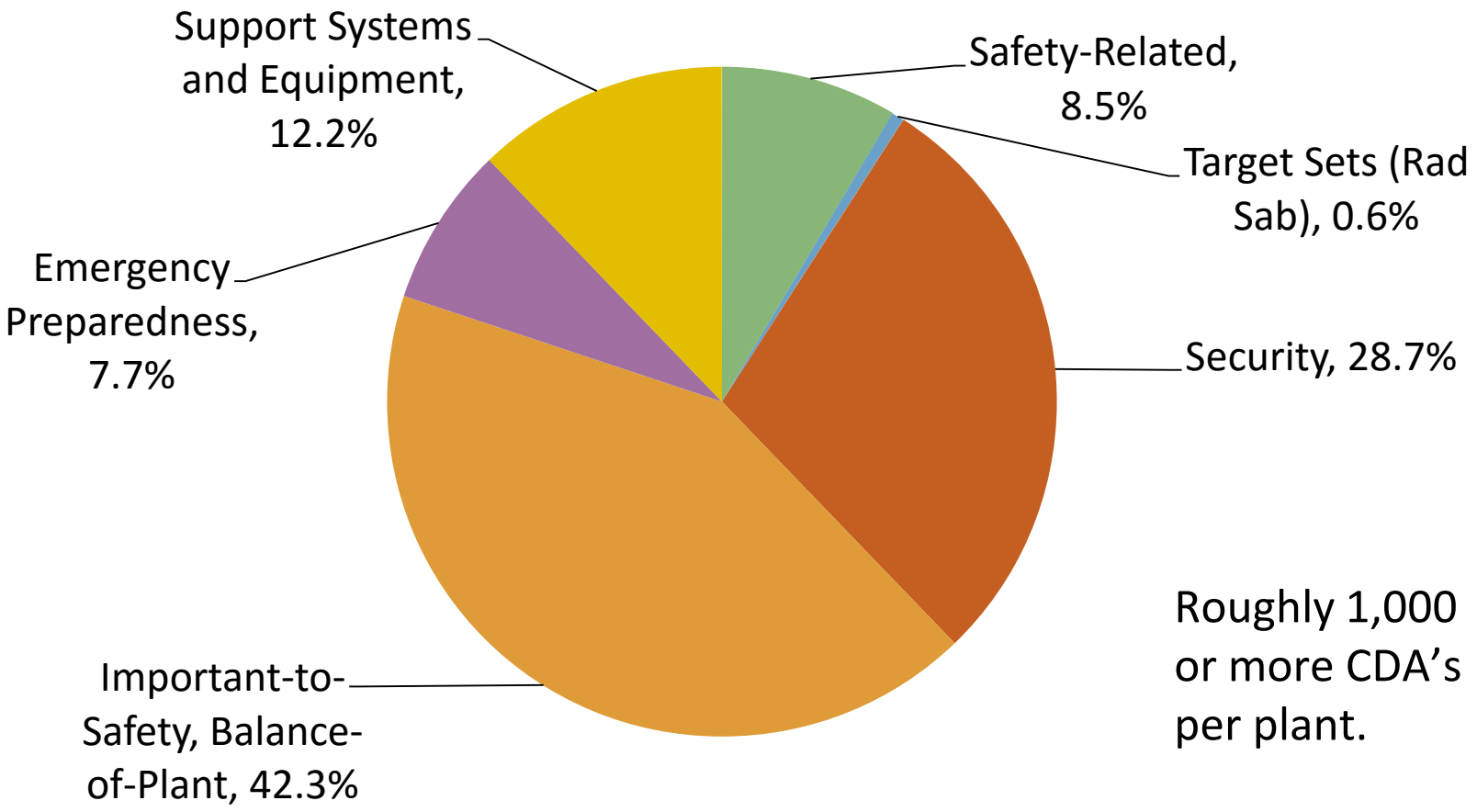
Program Scope, Performance Objectives

- The reactor cyber rule is disconnected from the performance objective of preventing radiological sabotage
- We are protecting against cyber attacks equipment that we do not protect against physical attacks
- This is a substantive issue of policy impacting ongoing rulemaking activities and must be addressed by the NRC

Design Basis Threat vs Assets Protected



Digital Asset Percentage by Function



Roughly 1,000 or more CDA's per plant.

The Internal Threat

- Internal threat is treated differently for cyber
  - Our mitigation programs are recognized as adequate to address physical acts by an insider
  - The same programs are not recognized as adequate to address cyber acts by an insider
- Insider mitigation programs were enhanced in 2010 to meet changes to 10 CFR Part 73.55 and 73.56 that addressed cyber concerns

Program Implementation

- There is no clear alignment between regulation, plan and commitments, and acceptance criteria
  - There should be line-of-sight across:
    Rule → Commitment → Acceptance Criteria
- Acceptance criteria were not established – standards were revealed during inspections
  - Challenged implementation and inspection

Program Implementation, Cont.

- NIST 800-53 was inappropriately used, causing significant implementation challenges
  - Not directly suited for industrial assets
  - Tailoring guidance was not incorporated
  - Was not filtered against existing requirements
- The program was not piloted to inform guidance, commitments, acceptance criteria
- Guidance is not risk-informed

Industry Support and Executive Oversight

- An industry executive-level steering group for cyber was not established early in the rulemaking process
- Industry and the CSTF did not take an active role in supporting station inspections
- Both activities could have improved implementation efficiency and supported issue identification and resolution

Inspections and NRC Oversight

- The use of good faith enforcement discretion was both beneficial and challenging
- Reliance on contractors was problematic
  - Considerable deference given during inspections
    - Applied a zero-risk mentality
  - May be attributed to a lack of acceptance criteria
- There were regional differences with respect to acceptable implementation

Summary

- Many lessons were learned that can be applied to ongoing or future rulemaking or implementation
- For power reactors, these lessons learned have, in general, been addressed
- The scope issue is a significant matter of policy that has not been satisfactorily addressed

End of Presentation